SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Emerging Issues >

Do Cyber and Corporate Security Work Together in Your Organization?

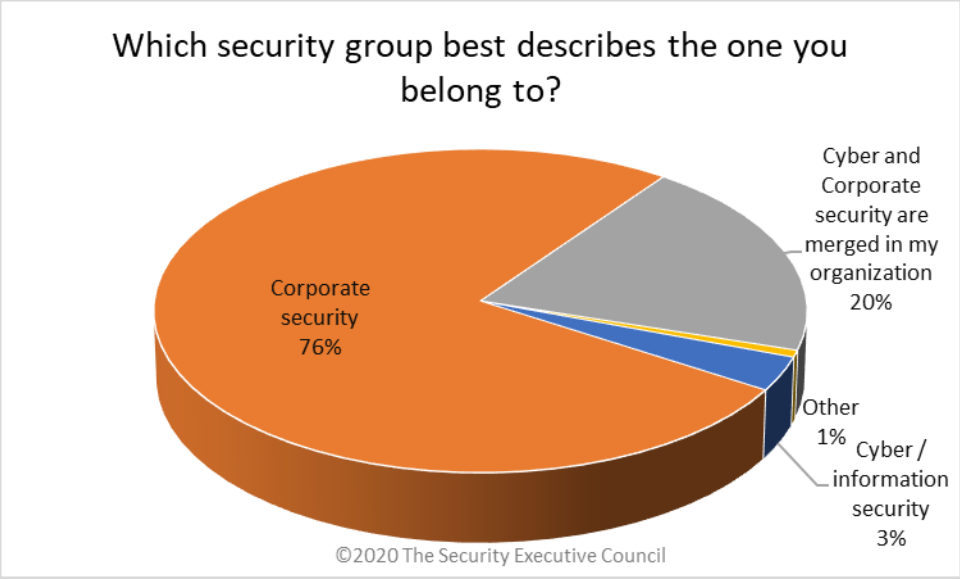
By the Security Executive Council

Both cyber/information security and corporate/physical security have roles to play in protecting and securing the organization. Some organizations approach these as two unique business silos and others see benefit in interaction and shared vision.

This research, conducted in partnership with our strategic alliance partner ISC2, investigated the extent of integration and cooperation between these two groups.

Demographics

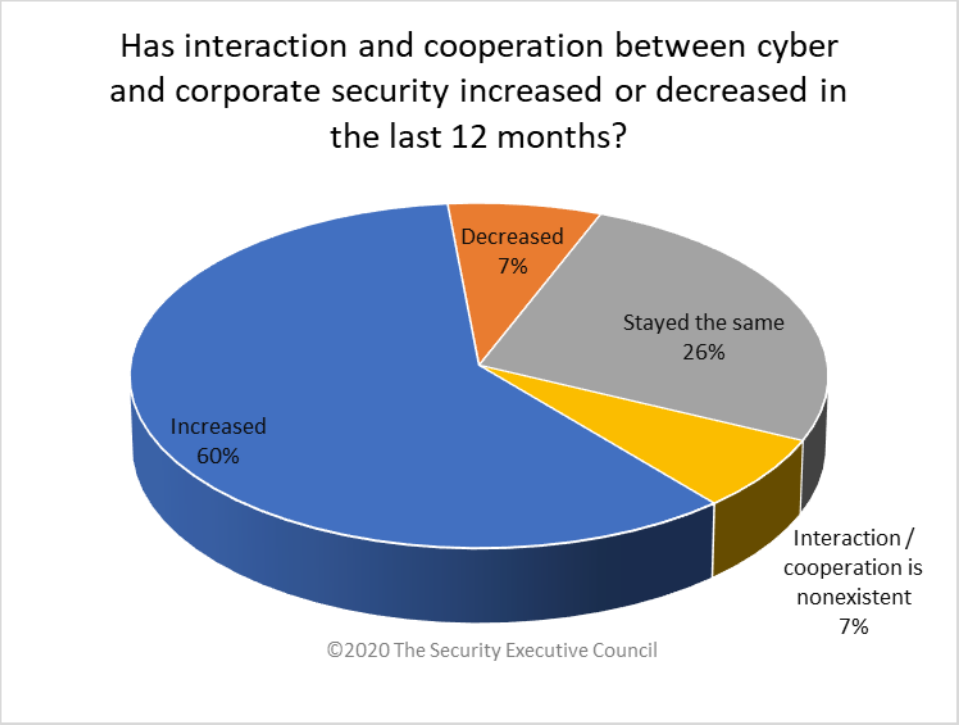
Roughly 76% of the survey respondents represented the corporate security group exclusively.



Was Cooperation Increasing or Decreasing?

We asked all participants if they felt interaction and cooperation between the groups was increasing or not over the past year.

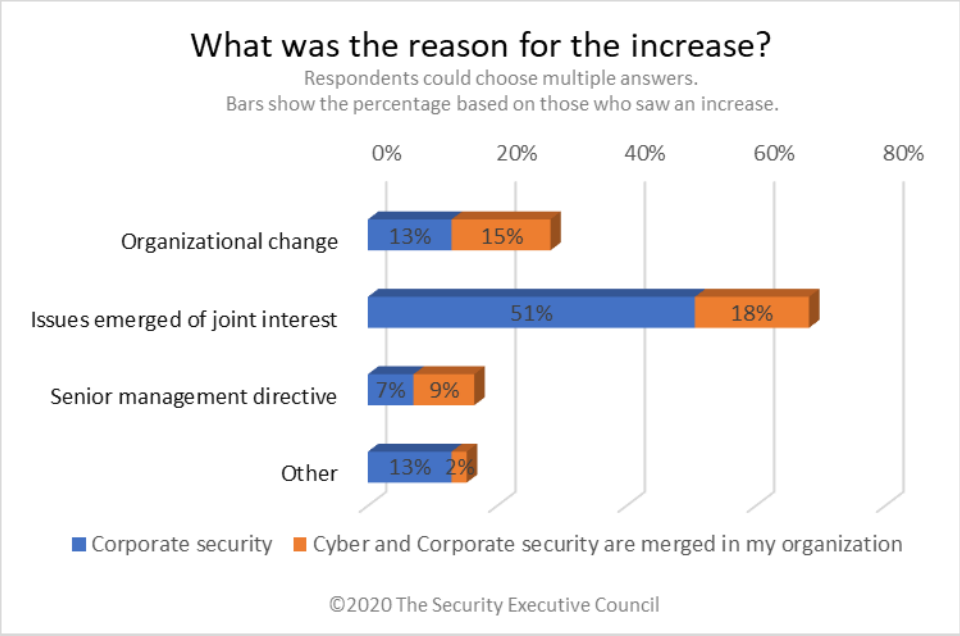
Roughly all respondents who represented cyber / information security or a mix of the two groups felt that interaction was increasing or staying the same. The responses among the participants exclusively representing the corporate security group were mixed. While 53% found interaction increasing, almost 20% felt that interaction had decreased or was non-existent.



Possible Reasons

We followed up by attempting to identify some of the reasons behind these responses.

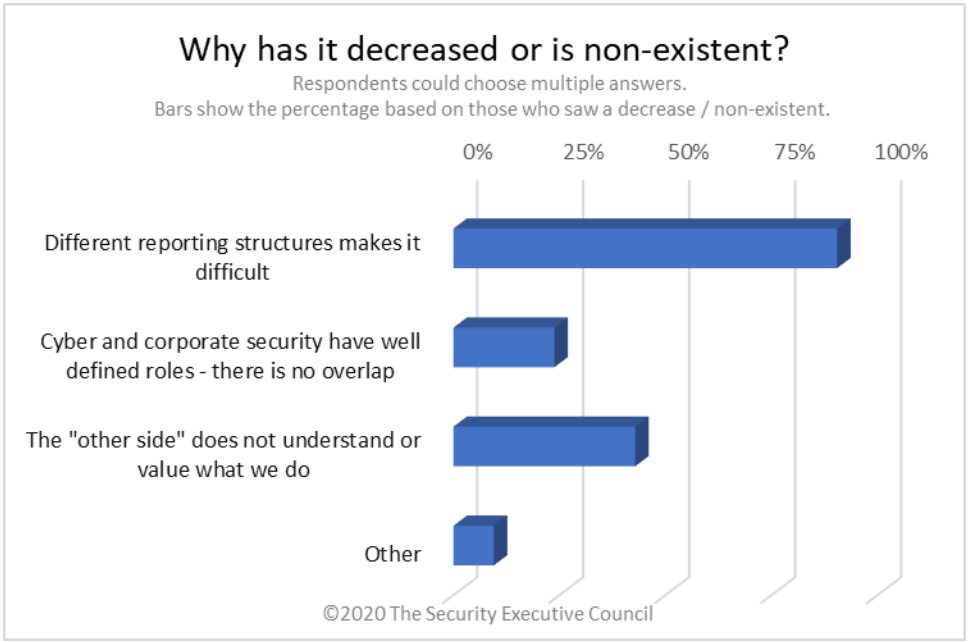
First, we focused on the reasons for an increase in cooperation and interaction. The most popular response was that emergent issues drove the increase in interaction.



We found some of the commentary regarding this question enlightening (comments were edited to preserve anonymity of respondents).

- *I came from a background that required a mutual appreciation for physical security and cyber security.*
- *Increase due to push from cyber/information specialist.*
- *A new role was created in the IT organization (NOT cyber) to help bridge the gap*
- *Meeting regulatory compliance.*
- *Elevation of CISO in organization as a result of cyber issues increasing in corporate perspective/brand protection.*
- *Intentionality by both groups to understand and leverage the value of working side by side.*
- *We created a working group to include Cyber, Physical Security and Insider Threat.*
- *Both groups agreed it made sense to begin to combine operations centers to share info.*
- *Increased focus on holistic risk management.*
- *Driving of collaborative effort on behalf of the Corp Security Team.*
- *Stronger personal relationships.*

We asked a similar question to those that felt interaction was decreasing or non-existent. (Note this group consisted of practitioners representing corporate security exclusively.)



Insightful Commentary Provided by Participants

We provided all participants with an opportunity to optionally provide additional commentary and/or explanation. We felt that there was additional insight to be gained by providing some selected responses (comments were edited to preserve anonymity of respondents).

- *During this unprecedent time Cyber and Corporate Security has been able to converge and work together to assess, manage, and prevent the emerging Covid-19 related crimes that represent the new security risk reality. Hopefully, this will stay as a lesson learned over and beyond Crisis Response and Management.*
- *Info Sec / cyber security and physical security go hand in hand and there needs to be close alignment when thinking about the appropriate mitigation to reduce / manage the risks. We are organizationally separate but have very strong relationships and a governance framework which holds us both to account. We are clear about roles and responsibilities, who leads and who supports.*
- *Both would think they were king, but both worlds do not understand each other and extremely underestimate their technical systems, integrations and their knowledge about the other and the adversaries. Only those who lived in both can really merge both.*
- *Physical and Cyber can't be seen as two silos in today's world. That's why we merged our departments.*
- *Cooperation slightly increased. Senior management is not fully aware about the benefits of increasing cooperation. However, on middle management level, we are aware and started cooperation in different fields.*
- *As the convergence of physical and cyber continues in the industry, I see companies struggling to make the cultural change that matches the threats. Risk managers are often valued by their ability to navigate both the CISO and CSO organizations and that will ultimately lead to a joint organization. Some companies are doing this faster than others.*
- *Unfortunately, until ALL security functions report up to a single point of leadership, response to security risks and incidents will remain compartmentalized. In our organization there are three "security" functions; Physical, cyber and privacy. They need an integrated team approach, but too often each one reports to a different leader with different budget priorities.*
- *We brought Privacy, Information Security, and Physical Security together at my company four years ago. While each area has unique functions, having all aligned under one umbrella organization has clearly improved the overall effectiveness and visibility of the programs. It has also improved efficiency and reduced costs through pooling resources in common areas like risk assessments, reporting, policy development, communications and training, administration, and program management. Our company leaders like having a one stop shop and our workforce likes hearing a consistent and integrated message.*
- *The CISO organization believed they should have governance over Corporate Security,*

mostly because the organization had historically undermined traditional security in structure, title, and importance to the organization. World events and the experienced, yet sizably smaller Corporate Security team has proven its ROI through its leadership in business continuity, security, and safety across the organization.

- *Corporate security is a department in corporate setup or organization that deals with matters of security and safety of property, people, and customers. Most business activities of organizations create interaction between various actors. Criminals exploit any opportunity arising from such activities and in most cases involve corporate staff and other actors. The medium of communication has shifted from the office to cyberspace. Security receives initial general complaints and categorize them accordingly. Cyber crimes are directed to the appropriate cyber security related personnel for further action. This creates a collaborative front between the cyber teams and security departments.*
- *Seems competitive. Cyber, Compliance, Audit, and regulatory authorities only see "physical security" as a minor component of cyber security.*
- *I appreciate our Cyber team's sincere efforts in collaborating more efficiently with corporate security and recognizing that our joint efforts are force multipliers in our work at protecting our organization.*
- *Although the two work streams complement each other, they exist entirely self-sufficient on a day to day basis. Many times, the work streams are so different that either team finds themselves in meetings where they have no action items.*
- *Cybersecurity and physical security converge, physical security is the first defense of information security.*
- *Largely stayed the same, but there have been minor changes. For instance, laptop theft / losses are now investigated by Corp Security and no longer by Cyber / info Security. We are now participating in third party studies led by Cyber Security that assess current state / gap analysis re: cyber security (smaller element of physical). Future opportunities to collaborate are being discussed, but still in development stages.*
- *We have our day-to-day independent verticals but largely work well together around shared risks.*
- *Everything security wise to include physical, BCP/DRM, risk management, security training and electronic ('cyber') is handled by the Security team. Corporate pays attention when there is enough money to put the client out of business. Otherwise we are a nuisance.*
- *Corporate Security introduced a Security & Privacy by Design throughout all business units and created Business Information Security Officers (BISO) for each business unit advocating that no new services must be released before going through the SPbD processes, Threat Assessment and Security Testing formally. This goes in line with worldwide Privacy legislation changes as well as growing the use of Opensource software use especially in Cloud computing environments i.e., Hybrid Cloud environments.*
- *With continued work from home at our sites, and heavier use of technology we need to partner and communicate more regarding media policy violations.*

- *Only a couple of years ago, within our company the cyber security was seen as "someone else's issue" by our security management, as there was a challenge of "kingdoms" and risk of being absorbed into a different reporting structure if the two were together. When that leadership changed approximately 2 years ago, a concerted effort was made to work much more collaboratively, while keeping the organizations separate. We recognized that the cyber teams perform vastly different functions (operationally) from operational security teams. It was also shown that the response capabilities for a cyber incident were good around identifying and responding internally, but sorely lacking in the investigative and evidentiary realm. There was a definite collaborative need on both sides. We kept the reporting structures separate but now work very closely and collaboratively with each other...mainly out of need.*
- *It is absolutely critical for cyber and corporate security to be working as one given the dynamic 360 threat environment.*
- *We have always been well connected. In our company there is a dedicated person in Industrial Security who works directly with the management of Cyber Security to co-ordinate response, initiatives, programs, and to share intel. That person has a dotted line reporting relationship with the Global CISO.*
- *The Covid-19 Pandemic has provided opportunities for even greater collaboration - which we have taken advantage of by assigning additional resources to support the joint mission and to learn from each other.*
- *Increased collaboration to review / align on future tech spend that support brand reputation and IP. 2) Initiation of a cross functional approach to establish an insider threat program*
- *Physical Security and InfoSec have looked for ways to continue our partnership. Some areas have included:*
    - *Adding infosec into physical security's risk assessment for travel support to include*
        - *device and access security practices*
        - *leveraging our GSOC supporting a process to alert infosec in the event that company-issued devices are lost or stolen*
    - *Partnering with InfoSec during investigations of lost or stolen devices.*
        - *I usually receive technical guidance prior to interaction with local investigators or law enforcement*
- *Work in progress, common cross over in technologies (OSNIT gathering), but differences in mission. Looking to collaborate more on exchange of information to track anomalies.*
- *Any forward leaning corporation must have a hand in hand relationship between IT And Corporate security. The company could not survive without it and personally I have made great efforts to keep this relationship strong and further work together. I have weekly meetings with the CIO and actually share one employee from IT who works 20 hrs with Corporate security and 20 hrs with IT. We experimented and it is working very well. The communications are superb. We have several training sessions together and coordinate closely and corporate security takes the lead on messaging cyber security awareness to all employees. We also work closely on cases as most of them do have cyber*

implications.

- *Although only minimal increased interaction, the organization recognizes that at some point, both realms of security diverge. Lateral coordination between the two has been more frequent of which may also be attributed to the hyperactivity brought about by the pandemic.*
- *Cyber and physical merged 1 year ago and fall under IT. It is not a good fit. Cyber and physical should work together closely but should not be merged.*
- *With the network monitoring of devices in our physical security GSOC, as well as the monitoring of the network equipment in the Cyber teams, there is a joint interest to understand status with our remote office locations, particularly when employee staffing levels are low during the coronavirus period. We've also upgraded our instant messaging tools across the company which makes it easier to collaborate with the cyber teams.*
- *We initiated a significant threat management tool that our facilities can report threats against the company or leaders within the company via social media accounts and emails. Together physical security and cyber investigate these threats. We are also looking at internal threats and risk mitigation efforts using security technology such as access control, computer login and security cameras to identify trends of employee workflow to determine nefarious acts (e.g. theft).*
- *Cyber security is not something merely computerized, nor should it be left to computer scientists. Cyber security is social networks, geopolitics, industrial espionage, police, phishing, human errors, industrial sociology ... that is why it must be directed by the corporate security direction, be one more leg of security, and directed by non-computer scientists.*
- *Security and Cyber Security are functional silos. What is accomplished together is pretty much dependent on the personalities of the two leaders and how well they get along with each other. There is no policy mandating they work together or requirement for measurement of their success if/when they do work together.*
- *Both groups belong to different organizations in our company but connect on related responsibilities. Usually Corp Security will assist with passing on any cyber related Intel, phishing complaints, technology theft, etc...*

Next Steps

The Security Executive Council can assist you with rationale, strategies, and communication vehicles to help increase interaction and cooperation between corporate and cyber security and other valuable partnerships across your organization. Contact Us to discuss your current situation and goals.

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations: Emerging Issues series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

